



***Cabinet for Health and Family Services (CHFS)
Information Technology (IT) Policy***



040.201 Internal Risk Assessment

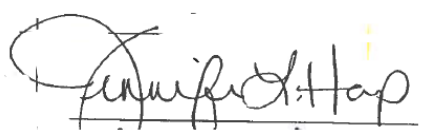

**Version 1.1
March 29, 2018**

040.201 Internal Risk Assessment	Current Version: 1.1
040.000 Contingency Planning/Operations	Review Date: 03/29/2018

Revision History

Date	Version	Description	Author
4/29/2016	1.0	Effective Date	CHFS IT Policies Team Charter
3/29/2018	1.1	Revision Date	CHFS OATS Policy Charter Team
3/29/2018	1.1	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
CHFS IT Executive (or designee)	3/29/2018	Jennifer Harp	
CHFS Chief Security Officer (or designee)	3/29/2018	DENNIS E. LEBER	

040.201 Internal Risk Assessment	Current Version: 1.1
040.000 Contingency Planning/Operations	Review Date: 03/29/2018

Table of Contents

040.201 INTERNAL RISK ASSESSMENT	5
1 POLICY OVERVIEW.....	5
1.1 PURPOSE	5
1.2 SCOPE	5
1.3 MANAGEMENT COMMITMENT.....	5
1.4 COORDINATION AMONG ORGANIZATIONAL ENTITIES	5
1.5 COMPLIANCE	6
2 ROLES AND RESPONSIBILITIES	6
2.1 CHIEF INFORMATION SECURITY OFFICER (CISO)	6
2.2 SECURITY/PRIVACY LEAD	6
2.3 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY OFFICER	6
2.4 CHFS STAFF AND CONTRACT EMPLOYEES	7
3 POLICY REQUIREMENTS	7
3.1 GENERAL	7
4 POLICY MAINTENANCE RESPONSIBILITY	7
5 POLICY EXCEPTIONS	7
6 POLICY REVIEW CYCLE.....	7
7 POLICY REFERENCES	8

040.201 Internal Risk Assessment	Current Version: 1.1
040.000 Contingency Planning/Operations	Review Date: 03/29/2018

Policy Definitions

- **Confidential Data:** Defined by COT standards, is data of which the Commonwealth has a legal obligation not to disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples would include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Critical Systems:** Any system or application that is federally mandated/regulated, deemed critical by the data or system owner(s), or deemed a “24 hours, 7 days a week, 365 days a year” (24x7x365) application, will be defined as a critical system. CHFS ITMP will be the source of knowledge and repository of severity level for systems/applications.
- **Major System Change:** Centers for Medicare and Medicaid Services (CMS) defines Major System Change to an information system as: installation of a new or upgraded operating system, middleware component, or application, modifications to system ports, protocols, or services, installation of a new or upgraded hardware platform, modifications to cryptographic modules or services, and/or modifications to security controls. Examples of significant changes to the environment of operation may include for example: moving to a new facility, adding new core missions or business functions, acquiring specific and credible threat information that the organization is being targeted by a threat source, and/or establishing new/modified laws, directives, policies, or regulations.
- **Risk:** An adapted definition from NIST SP 800-30 is the net mission impact considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur. Risks arise from legal liability or mission loss due to: (a) Unauthorized (malicious or accidental) disclosure, modification, or destruction of information; (b) Unintentional errors and omissions; (c) IT disruptions due to natural or man-made disasters; (d) Failure to exercise due care and diligence in the implementation and operation of the IT system.
- **Risk Assessment:** The overall process of risk analysis and risk evaluation.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver’s license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **Threat:** Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations or the Commonwealth through an information system via unauthorized access, destruction, disclosure or modification of information and/or denial of service.

040.201 Internal Risk Assessment	Current Version: 1.1
040.000 Contingency Planning/Operations	Review Date: 03/29/2018

040.201 Internal Risk Assessment

Category: 040.000 Contingency Planning/Operations

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a risk assessment policy. This document establishes the agency's Internal Risk Assessment (RA) Policy which helps manage risk and provides guidelines for security best practices regarding risk assessments, preparation, and strategy.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors or other defined groups/organizations providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restricted access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within the cabinet with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted with OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking an exception to this policy.

040.201 Internal Risk Assessment	Current Version: 1.1
040.000 Contingency Planning/Operations	Review Date: 03/29/2018

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This position is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This designated position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role along with the CHFS OATS Information Security (IS) Team is responsible for the adherence of this policy.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS Information Security (IS) Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO, or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position is responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notifications in accordance with HIPAA rules and regulations.

040.201 Internal Risk Assessment	Current Version: 1.1
040.000 Contingency Planning/Operations	Review Date: 03/29/2018

2.4 CHFS Staff and Contract Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3 Policy Requirements

3.1 General

The CHFS agencies will assess the risk to information systems confidentiality, integrity, and availability through the execution of Risk Assessments. These assessments will be conducted in accordance with the NIST 800-30 Revision 1, Risk Management Framework (RMF) and the HIPAA Security Rule, 45CFR164.308(a)(1)(ii)(A).

All new application and system development must have a Risk Assessment conducted prior to inception, at the time of any major system change, and at least once annually. All Risk Assessments shall incorporate a corresponding risk mitigation plan created to reduce threats and vulnerabilities identified.

Additional guidelines for Risk Assessments can be found within the Enterprise CIO-093 Risk Assessment Policy, Enterprise CIO-082Critical Systems Vulnerability Assessments Policy, and the CHFS Risk Assessment Program Procedure.

4 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

5 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

6 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

040.201 Internal Risk Assessment	Current Version: 1.1
040.000 Contingency Planning/Operations	Review Date: 03/29/2018

7 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS OATS Procedure: Risk Assessment Program Procedure
- Enterprise IT Policy: CIO-082 Critical Systems Vulnerability Assessments Policy
- Enterprise IT Policy: CIO-093 Risk Assessment Policy
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45CFR164.308(a)(1)(ii)(A)
- Information Technology Management Portal (ITMP)
- Internal Revenue Services (IRS) Publication 1075
- National Institute of Standards and Technology (NIST) Special Publication 800-30 Revision 1, Risk Management Guide for Information Technology Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information